Privacy and Confidentiality Policy

Section 1 - Preamble

(1) This document sets out a framework for the protection of personal privacy and confidentiality consistent with the University's obligations and commitment to protecting the privacy of all members of the University community.

(2) The University will act responsibly to collect, manage, use and disclose personal information in accordance with the Northern Territory Information Act 2002.

Section 2 - Purpose

(3) This policy provides guidance and principles for the protection of personal privacy and information as required by the Information Act 2002 and other legislative instruments, including how to handle international responsibilities such as those under the European Union's General Data Protection Regulation.

Section 3 - Scope

(4) All staff of the University and other members of the University community who are responsible for the collection, handling, storage, disposal and access to personal and confidential information must be aware of their responsibilities under the Information Act 2002. This policy also applies to those members of the University staff and community who incidentally collect such information as part of or outside their normal duties.

Section 4 - Policy

Collection of Personal Information

(5) The University will only collect personal information that is necessary for one or more of its functions or activities.

(6) The University will only collect personal information in a lawful, fair and not unreasonably intrusive way.

(7) When personal information is collected from an individual, the University will take reasonable steps to ensure that the individual is:

a. Aware of the University's identity and how to contact it;
b. Able to have access to the information;
c. Aware of the purpose for which the information is collected;
d. Aware of the persons or bodies, or classes of persons or bodies, to which the University usually discloses personal information;
e. Aware of any law that requires the collection of the information; and
f. Aware of any consequences for the individual if they do not provide all or part of the information.

(8) If it is reasonable and practical to do so, the University will only collect personal information about an individual

from that individual. If the University collects personal information about an individual from another person, it will take reasonable steps to ensure the individual is or has been made aware of the matters listed above unless making the individual aware of these matters would pose a serious threat to the life or health of a person.

(9) The University may use and disclose personal information only in the following instances, after a written note of the use or disclosure is made:

a. The use or disclosure is related or directly related to the purpose for collecting it and the individual would reasonably expect the University to use or disclose it for that purpose;
b. with the individual's consent;
c. the use or disclosure is necessary for research or the compilation or analysis of statistics in the public interest, and:
    i. only where the research will not be published in identifiable form; and
    ii. the individual's consent cannot be reasonably obtained; and
    iii. the recipient of the information will not disclose the personal information; and
    iv. where any health information is only used or disclosed in accordance with guidelines issued by the Information Commissioner under section 86(1)(a)(iv) of the Information Act 2002.
d. to lessen or prevent a serious and imminent threat to a person's life, health or safety, or of harm to or exploitation of a child, or serious threat to public health or safety;
e. when required in the investigation or reporting of unlawful activity, or assisting a law enforcement agency;
f. where the use or disclosure is required or authorised by law; or
g. in connection with the performance of the functions of the Australian Security Intelligence Office (ASIO) or Australian Secret Intelligence Service (ASIS) where authorised in writing.

Trans-border Data Flows

(10) The University will not transfer personal information about an individual to a person (other than the individual) outside the Northern Territory unless:

a. the transfer is required or authorised under a law of the Northern Territory or the Commonwealth; or
b. the University reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to the Information Privacy Principles and Australian Privacy Principles; or
c. the individual consents to the transfer; or
d. the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request; or
e. the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or
f. all of the following apply:
    i. The transfer is for the benefit of the individual;
    ii. It is impracticable to obtain the consent of the individual to the transfer;
    iii. It is likely that the individual would consent to the transfer; or

(11) The organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred, in a manner that is inconsistent with the Information Privacy Principles or Australian Privacy Principles.

(12) The University will ensure that any contracts with third parties where personal information may

be transferred, contain privacy clauses requiring compliance with the Information Act 2002 and the Information Privacy Principles and/or the Privacy Act 1988 and the Australian Privacy Principles.

Data Quality

(13) The University will take all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Data Breaches

(14) The Notifiable Data Breach Scheme, as detailed in the Privacy Act 1988 requires regulated entities to notify affected individuals and the Australian Information Commissioner about the occurrence of eligible data breaches.

(15) As soon as possible after the breach has occurred, all suspected eligible data breaches must be referred to the University's Privacy Officer for actioning and reporting as they deem appropriate.

Information Security

(16) The University will protect all personal information it holds from misuse, loss, unauthorised access, modification or disclosure by:

a. Implementing industry standards for the security and protection of personal information; and
b. Storing information in either electronic and/or hard copy forms with access restricted to authorised personnel only.

(17) Security, integrity and accuracy of information is governed by the University's Information and Communication Technologies Acceptable Use Policy, Information Security and Access Policy, and Records and Information Management Policy and Procedure.

(18) The University will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose in accordance with the Retention and Disposal Schedules.

Privacy and Confidentiality Obligations

(19) Staff members, students, researchers, contractors and any other third party who collect use or disclose personal information on behalf of the University have a responsibility to act consistent with the Information Privacy Principles and Australian Privacy Principles and to take appropriate measures to avoid a breach of confidence.

(20) Under the Higher Education Support Act 2003, it is an offence (punishable by fine or imprisonment), if a staff member of the University discloses, copies or records personal information otherwise than in the course of official employment, or causes unauthorised access to or modification of personal information held by the University.

(21) At any time during and after employment with the University, staff members must not use, divulge, copy or communicate any confidential information to any person without the University's consent, regardless of whether the other person is an employee of the University or not, except as required in the ordinary performance of the staff member's duties.

(22) Unauthorised access to personal information must be reported to the University's Privacy Officer and, where relevant, to the responsible owner of the information system concerned. Failure to comply with this Policy may necessitate disciplinary action.

(23) University matters relating to individuals or non-public information must not be discussed, except where directly related to the staff member's role, as this may constitute a breach of confidence and therefore misconduct.

Information and Communication Technologies Facilities

(24) Users of the University's Information and Communication Technologies (ICT) facilities are reminded that anything that is written or recorded is potentially subject to subpoena or Freedom of Information requests or other authorised access. Inappropriate use of the University's Information and Communication Technologies (ICT) facilities may be subject to disciplinary action.

General Data Protection Regulation (GDPR)

(25) The General Data Protection Regulation (GDPR) is the privacy law of the European Union (EU) that took effect from 25 May 2018 and applies to all EU and European Economic Area (EEA) member states. It also applies to the United Kingdom post-Brexit, as the UK has retained the GDPR in UK law and will continue to be read alongside the Data Protection Act 2018 (UK).

(26) The GDPR covers the personal data of all-natural persons within the EU/EEA and UK ("EU/EEA and UK data subjects"). The GDPR makes no distinctions based on an individual's permanent place of residence or nationality. The GDPR applies to all such individuals' personal data.

(27) The GDPR also applies to the processing of personal data by data controllers or data processors who are not based in the EU/EEA and UK, where they process personal data of individuals in the EU/EEA and UK in connection with the offering of goods/services.

(28) EU/EEA and UK data subjects have additional rights under the GDPR, including that they are entitled (subject to the requirements and constraints of the GDPR) to:

a. access the personal data the University holds about them, and to receive that personal data in a structured, commonly used and machine-readable format;
b. raise an objection to decisions made by the University based on automated processing of personal data, where the processing of personal data the University holds about them is likely to significantly affect him or her;
c. request either the rectification of any incorrect, incomplete or outdated personal data or restrict further processing of that individual's personal data;
d. request erasure of their data (right to be forgotten) and this must be undertaken by the University without undue delay; and
e. require that their personal data not be processed for the purpose of direct marketing.

Access and Correction

(29) On the request of an individual, the University will take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.

(30) On the request of an individual, the University will provide access to their personal information, except to the extent that:

a. providing access would pose a serious threat to the life or health of the individual or another individual; or
b. providing access would prejudice measures for the protection of the health or safety of the public; or
c. providing access would unreasonably interfere with the privacy of another individual; or
d. the request for access is frivolous or vexatious; or
e. the information relates to existing or anticipated legal proceedings between the University and the individual and the information would not be accessible by the process of discovery or subpoena in those proceedings; or
f. providing access would reveal the intentions of the University in relation to negotiations with the individual

in such a way that would prejudice the negotiations; or

g. providing access would be unlawful; or
h. denying access is required or authorised by law; or
i. providing access would be likely to prejudice an investigation of possible unlawful activity; or
j. providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:
    i. preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
    ii. enforcing a law relating to the confiscation of proceeds of crime;
    iii. protecting public revenue;
    iv. preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
    v. preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or
k. providing access would prejudice:
    i. the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or
    ii. the maintenance of law and order in the Territory.

(31) However, where providing access would reveal evaluative information generated within the University in connection with a commercially sensitive decision-making process, the University may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

(32) If the University holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the University will take reasonable steps to correct the information so that it is accurate, complete and up to date.

(33) If an individual and the University disagree about whether personal information about the individual held by the University is accurate, complete or up to date; and

a. The individual requests the University to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date;
b. The University will take reasonable steps to comply with that request.

(34) The University will provide reasons for refusing to provide access to or correct personal information.

(35) If an individual requests the University for access to, or to correct personal information held by the University, the University will, within a reasonable time:

a. Provide access or reasons for refusing access; or
b. Make the correction or provide reasons for refusing to make it; or
c. Provide reasons for the delay in responding to the request;

(36) If the University charges a fee for providing access to personal information, the fee will not be excessive. Access and amendment requests should be directed to the University's Privacy Officer.

Notification of correction to third parties

(37) If the University corrects personal information that the University previously disclosed to another entity, and the individual requests the University to notify the other entity of the correction, the University will take such steps as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Sensitive Information

(38) The University will not collect sensitive information about an individual unless:

a. the individual consents to the collection; or
b. the University is authorised or required by law to collect the information; or
c. the individual is:
    i. physically or legally incapable of giving consent to the collection; or
    ii. physically unable to communicate his or her consent to the collection; and
    iii. collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or
d. collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

(39) However, the University may collect sensitive information about an individual if:

a. the collection:
    i. is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
    ii. is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and
b. there is no other reasonably practicable alternative to collecting the information for that purpose; and
c. it is impracticable for the organisation to seek the individual's consent to the collection.

Section 5 - Non-Compliance

(40) Non-compliance with Governance Documents is considered a breach of the Code of Conduct – Staff or the Code of Conduct – Students, as applicable, and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures outlined in the Charles Darwin University and Union Enterprise Agreement 2025 and the Code of Conduct – Students.

(41) Complaints may be raised in accordance with the Code of Conduct – Staff and Code of Conduct - Students.

(42) All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Policy and Whistleblower Reporting (Improper Conduct) Procedure.

Status and Details

Status	Historic
Effective Date	15th January 2022
Review Date	23rd June 2024
Approval Authority	University Council
Approval Date	24th June 2021
Expiry Date	12th December 2024
Responsible Executive	Brendon Douglas Vice-President Governance and University Secretary
Implementation Officer	Brendon Douglas Vice-President Governance and University Secretary
Enquiries Contact	Brendon Douglas Vice-President Governance and University Secretary